

معرفی ProtonMail: حریم خصوصی و امنیت

دهه‌ها از ظهور ایمیل می‌گذره؛ همچنان ازش استفاده می‌کنیم، و در بعضی موارد بهش وابسته‌ایم. اما خوبی دوره‌ای که در اون زندگی می‌کنیم اینه که امروز گزینه‌هامون بیشتر از سرویس‌های متداولی مثل یاهو و جی‌میلن.

در اینجا به معرفی و آموزش استفاده از سرویس پروتون‌میل خواهیم پرداخت.



شاید قبل از پرداختن به موضوع اصلی جالب باشه پیش‌زمینهٔ کوچکی درمورد تاریخچهٔ ایمیل پیدا کنیم. از ریموند تاملینسون به‌عنوان سازندهٔ ایمیل و کسی که اولین پیام رو از یک کامپیوتر به کامپیوتر دیگری در شبکه ارسال کرد یاد می‌شه. این موضوع به سال ۱۹۷۱ برمی‌گرده—پنجاه سال پیش در زمان نگارش این مطلب.

INDIEGOGO





CLOSED

ProtonMail

Swiss based encrypted email, protecting privacy rights for everyone.

Andy Yen
1 Campaign | Geneva, Switzerland

$550,377 USD 10,576 backers



550% of $100,000 Flexible Goal

FOLLOW



کمپین جذب سرمایهٔ جمعی پروتون‌میل در Indiegogo

تاریخچهٔ پروتون‌میل

در مهٔ ۲۰۱۴، پروتون‌میل با هدف ارائهٔ حریم خصوصی بیشتر به کاربرها کار خودش رو شروع کرد. استقبال به‌قدری زیاد بود که در انتهای ژوئیه، تنها دو ماه بعد، در کمپین جذب سرمایهٔ جمعی‌شون به مبلغ باورنکردنی نیم میلیون دلار رسیدن، درحالی‌که هدف اولیه ۱۰۰,۰۰۰ دلار بود.

پروتون‌میل، که استفاده ازش در ابتدا نیازمند دریافت دعوت‌نامه بود، مارس ۲۰۱۶ عمومی شد، و کاربرها حالا می‌تونستن بدون محدودیت از این سرویس استفاده کنن. چند ماه بعد، شاهد جهشی در تعداد کاربران ایرانی بودیم، و از اون زمان تا امروز تنها می‌شه تصور کرد این تعداد چقدر بیشتر شده.

اما پیش از اینکه بررسی کنیم چرا پروتون‌میل نسبت به سرویس‌های دیگه بهتره (و نه راه‌حل نهایی)، باید درنظر داشت که ایمیل راه ارتباطی امنی نیست. روش‌های بسیار امن‌تری وجود دارن. اگه مجبورید از ایمیل استفاده کنید و به امنیت و حریم خصوصی اهمیت می‌دید، بهتره از ایمیل‌های موقت (temporary email) استفاده کنید.

ضرورت حریم خصوصی در ارتباطات

افرادی که سعی در نقض حریم خصوصی شما دارن، از ابرشرکت‌ها گرفته تا سازمان‌های اطلاعاتی و حکومت‌ها، هیچ‌کدوم موفق به دسترسی به دادهٔ شما نخواهند شد اگه از رمزنگاری سرتاسر استفاده کنید. ایالات متحده از دهۀ ۱۹۹۰ تا امروز درتلاش بوده شرکت‌ها رو به ساخت در پشتی (backdoor) وادار کنه. درمورد تراشهٔ کلیپر (۱۹۹۳) بخونید، یا افشاگری‌های ادوارد اسنودن در ۲۰۱۳.

جف شیلر از MIT در مقاله‌ای در سال ۱۹۹۹ چه دقیق گفت، «ما نباید تکنولوژی نظارت رو درون استانداردها جا بی‌اندازیم. اجرای قانون قرار نبود آسون باشه. جایی که آسونه، بهش حکومت پلیسی (سرکوب‌گر) می‌گن.»



#ICYMI: During a congressional hearing this week, #FBI Director Christopher Wray discussed how end-to-end encryption threatens the FBI’s mission to protect the American people from federal crimes, including crimes against children, cyberattacks, and terrorism.



مشاهدهٔ ویدئو در توئیتر

توجه داشته باشید که رمزنگاری سرتاسر بین دو کاربر پروتون‌میل به‌طور پیش‌فرض اتفاق می‌افته. وقتی برای یک کاربر جی‌میل پیامی ارسال می‌کنید، گوگل به محتوای پیام شما دسترسی داره. درنتیجه، برای امنیت و حریم خصوصی بالاتر، بهتره افرادی که باهاشون ارتباط دارید از پروتون‌میل استفاده کنن.



دفتر مرکزی Proton Technologies در ژنو، سوئیس

تأسیس شرکت در سوئیس

یکی از برتری‌های احتمالی پروتون‌میل در تصمیمشون برای تأسیس شرکت و قراردادن مراکز داده‌شون در سوئیسه. از نظر قانونی، سوئیس خارج از حوزهٔ قضایی اروپا و آمریکاست، و سازمان‌های اطلاعاتی این کشورها بدون دریافت مجوزی از دادگاه سوئیس امکان دسترسی به داده‌های این شرکت رو ندارن. حتی دراون‌صورت، تنها چیزی که پروتون‌میل می‌تونه دراختیار اون‌ها بذاره ایمیل‌های رمزنگاری‌شده‌ست.

توجه مهم: باوجودی‌که پروتون‌میل ادعا می‌کنه اجباری در دراختیارقراردادن دادهٔ کاربرها نداره و، حتی درصورت درخواست، داده‌ای برای ارائه نداره، در زمان نگارش این مطلب و به دستور دستگاه قضایی سوئیس آدرس آی‌پی یک فعال فرانسوی رو ثبت کرد درحالی‌که تا پیش از این ادعا داشت هرگز چنین کاری نمی‌کنه. بنیان‌گذار پروتون، اندی ین، در توئیتی نوشته، «پروتون باید از قوانین سوئیس پیروی کنه.» به‌نظر میاد سوئیس تنها استثنا باشه، اما مهمه که درنظر بگیرید چرا قصد استفاده از پروتون‌میل رو دارید و آیا با مدل تهدید شما سازگاره یا نه. استفاده از وی‌پی‌ان **ضروریه**.

```
50      - **IP Logging:** By default, we do not keep permanent IP logs in relation with your use of the Services. However, IP
          logs may be kept temporarily to combat abuse and fraud, and your IP address may be retained permanently if you are
          engaged in activities that breach our terms and conditions (spamming, DDoS attacks against our infrastructure, brute
          force attacks, etc). The legal basis of this processing is our legitimate interest to protect our Services against
          nefarious activities.
    50  + **IP Logging:** By default, we do not keep permanent IP logs in relation with your use of the Services. However, IP
          logs may be kept temporarily to combat abuse and fraud, and your IP address may be retained permanently if you are
          engaged in activities that breach our terms and conditions (spamming, DDoS attacks against our infrastructure, brute
          force attacks, etc). The legal basis of this processing is our legitimate interest to protect our Services against
          nefarious activities. If you are breaking Swiss law, ProtonMail can be legally compelled to log your IP address as
          part of a Swiss criminal investigation. This obligation however does not extend to ProtonVPN ([see VPN privacy policy
          here](https://protonvpn.com/privacy-policy)). Additional details can be found in our [transparency report]
          (https://protonmail.com/blog/transparency-report).
```

تغییر اخیر در سیاست حریم خصوصی پروتون‌میل، که توسط Open Terms Archive گزارش شد

چرا پروتون‌میل؟

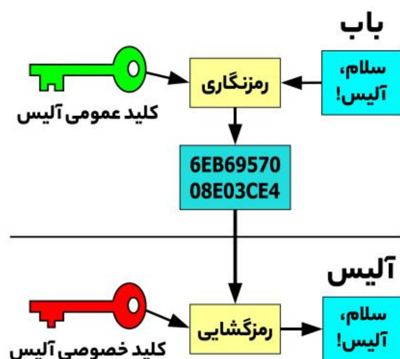
یکی از اصلی‌ترین تفاوت‌های پروتون‌میل با دیگر سرویس‌ها در اینه که کنترل دادهٔ شما در دست شماست. برعکس ابرشرکت‌هایی مثل گوگل و فیسبوک که مدل کسب‌وکارشون به دسترسی هرچه‌بیشتر به اطلاعات کاربرها وابسته‌ست، پروتون‌میل طوری طراحی شده که، حتی اگه بخواد، نمی‌تونه دادهٔ شما رو ببینه.



رمزنگاری سرتاسر در پروتون‌میل

وقتی از رمزنگاری سرتاسر برای ارسال پیام یا ایمیل استفاده می‌کنید، هیچ‌کسی این بین قادر به رمزگشایی و دیدن محتوای پیام شما نیست—نه اشخاص سوم، نه حکومت‌ها، و نه حتی پروتون‌میل که مکالمهٔ شما رو ممکن کرده. این رو با امکان انقضای پیام ترکیب کنید، و دیگه عالیه.

برای درک بهتر رمزنگاری سرتاسر به مثال روبه‌رو توجه کنید. در ادامه به توضیح جزئیات اون خواهیم پرداخت. درصورتی‌که با مفاهیم رمزنگاری آشنا نیستید، راهنمای رمزنگاری کلید عمومی RSA شروع خوبی برای شماست. بدون‌شک، بعد از مطالعه‌ش، موضوع‌های مرتبط با رمزنگاری رو بهتر درک خواهید کرد.



استفاده از رمزنگاری کلید عمومی

باب و آلیس می‌خوان خصوصی و امن با هم صحبت کنن. باب پیام خودش رو با **کلید عمومی آلیس** رمزنگاری می‌کنه، و در این فرآیند، «سلام، آلیس!» به متن رمزنگاری‌شده‌ای (ciphertext) تبدیل می‌شه، که از دید دیگران غیرقابل‌فهمه—EB6957008E03CE46.

باب، سپس، پیام رمزنگاری‌شدهٔ خودش رو ارسال می‌کنه. این پیام ممکنه از سرورهای مختلفی عبور کنه تا به مقصد برسه. در این بین، شرکت‌های واسطه ممکنه سعی کنن محتوای پیام رو بخونن، اما تبدیل متن رمزنگاری‌شده به متن آشکار (plaintext) بدون داشتن کلید خصوصی مرتبط غیرممکنه. درمقابل، آلیس (و تنها آلیس)، که کلید خصوصی خودش رو داره، بعد از دریافت پیام می‌تونه اون رو رمزگشایی کنه و بخونه.



وقتی آلیس می‌خواد پاسخی برای باب ارسال کنه، همین فرآیند رو تکرار می‌کنه: پیامش رو با **کلید عمومی باب** رمزنگاری و اون رو ارسال می‌کنه. تنها باب قادر به خوندنش خواهد بود.

برتری‌ای که رمزنگاری سرتاسر به میز میاره اینه که دادهٔ شما در مقابل نشت (leak) امنه. با فرض اینکه اشخاصی به داده‌های پروتون‌میل دست پیدا کنن، قادر به خوندن اون‌ها نخواهند بود چون کلید رمزگشایی اون‌ها دست هر کاربره. حتی پروتون‌میل هم از محتوای پیام‌های ردوبدل‌شده بی‌اطلاعه.

ارسال ایمیل به کاربران غیرپروتون‌میل

شما می‌تونید ایمیل‌هایی رو هم که برای کاربرهای دیگه ارسال می‌کنید رمزنگاری کنید، با یک قدم ساده: برای پیام رمز تعیین کنید و سرنخی (hint) بذارید که فقط طرف مقابل خواهد دونست. این پیام‌ها به‌طورپیش‌فرض بعد از بیست و هشت روز منقضی می‌شن. تاریخ انقضا رو می‌تونید دستی هم وارد کنید. به تصاویر زیر توجه کنید.

چند نکته در باب انقضای پیام‌ها

فقط پیام‌های رمزنگاری‌شده امکان انقضا دارن: ۱) بین دو کاربر پروتون‌میل؛ ۲) رمزنگاری‌شده برای کاربران غیرپروتون‌میل. تاریخ انقضا به محض زدن گزینهٔ ارسال شروع می‌شه، نه از زمان خوندن پیام توسط گیرنده، و بیشترین زمان انقضا چهار هفته‌ست (بیست و هشت روز).

رمزنگاری zero-access

پروتون‌میل از روشی با عنوان رمزنگاری zero-access استفاده می‌کنه. با این نوع رمزنگاری، حتی اگه داده‌ها لو یا به‌سرقت برن، قابل‌رمزگشایی نخواهند بود. برای درک تفاوت رمزنگاری zero-access و رمزنگاری سرتاسر به این سناریو توجه کنید.

وقتی از سرویسی غیر از پروتون‌میل—برای مثال، جی‌میل—پیامی دریافت می‌کنید، سرورهای پروتون‌میل به فاصلهٔ رسیدن ایمیل و رمزنگاری‌اش می‌تونن اون رو بخونن چون جی‌میل از رمزنگاری سرتاسر پشتیبانی نمی‌کنه. اما به محض دریافت ایمیل، پروتون‌میل اون رو با کلید عمومی کاربر رمزنگاری و سپس نگهداری می‌کنه. ازاون‌پس، پروتون‌میل هرگز قادر به رمزگشایی اون پیام نخواهد بود، و تنها کسی که این امکان رو داره خود کاربره. به این روش رمزنگاری zero-access می‌گیم.

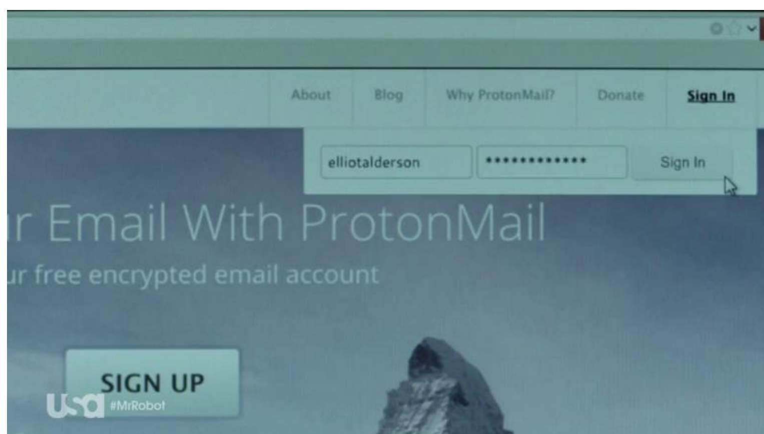
درمقابل، وقتی برای کاربر پروتون‌میل دیگه‌ای ایمیل ارسال می‌کنید، اون پیام روی دستگاه شما و با کلید عمومی گیرندهٔ پیام رمزنگاری می‌شه، قبل از اینکه بخواد به دست پروتون‌میل برسه. درنتیجه، تنها فرستنده و گیرنده از محتواش باخبرن. این رمزنگاری سرتاسره.

بین رمزنگاری سرتاسر و رمزنگاری zero-access، اولی قوی‌تره از این جهت که پروتون‌میل به‌هیچ‌عنوان امکان دیدن پیام رو نداره. رمزنگاری zero-access از اصل دادهٔ شما درصورت نشت یا سرقت محافظت می‌کنه، اما برای کسری از ثانیه (فاصلهٔ رسیدن پیام تا رمزنگاری) اون رو برای پروتون‌میل قابل‌دسترس می‌کنه. به‌همین‌خاطر، اگه پیامی با حساسیت بالا دارید، توصیه می‌شه دو طرف پروتون‌میل داشته باشن.

توجه کنید که پروتون‌میل یک ابزاره. فرقی نمی‌کنه که در سوئیسه. فرقی نمی‌کنه که ادعا می‌کنه امنیت و حریم خصوصی بهتری ارائه می‌ده. درنهایت، شما، به‌عنوان کاربر، در استفادهٔ کارآمد ازش مسئولید.

مستر ربات

قبل از اینکه به جزئیات روش رمزنگاری پروتون‌میل بپردازم، دوست دارم گذری به سریال مستر ربات داشته باشیم. این مجموعه، که داستان شخصی به نام الیوت رو دنبال می‌کنه، یکی از واقع‌گرایانه‌ترین آثاریه که می‌تونید درمورد امنیت، هک، و دنیای کامپیوتر ببینید. (این یک نظر شخصی نیست.)



صفحهٔ ورود پروتون‌میل در سریال مستر ربات (فصل اول، قسمت هشتم)

در فصل اول مستر ربات، الیوت رو می‌بینیم که از پروتون‌میل استفاده می‌کنه. این جزئیات در نگاه اول کوچک و کم‌اهمیت به‌نظر میاد، اما داستان پشتش و مکالمه‌های مفصلی که سازندگان سریال با تیم پروتون‌میل دراین‌باره داشته‌ن نشون از توجه بالا به واقع‌گرایی و کیفیت بی‌نظیر نتیجهٔ نهایی داره.

قسمت هشتم اوت ۲۰۱۵ به‌نمایش دراومد. از قول تیم پروتون‌میل، وقتی سازندگان مستر ربات در ژوئن باهاشون تماس گرفتن، از این سطح از تحقیق برای پیداکردن سرویس ایمیل امنی که شخصیتی مثل الیوت—یک هکر و متخصص امنیت—ازش استفاده کنه تعجب کردن. به‌راحتی می‌تونستن این جزئیات ریز رو نادیده بگیرن. اما داستان به اینجا ختم نمی‌شه، و همکاری این دو تیم به جاهای بسیار خوبی می‌رسه. سازندگان سریال به این نکته اشاره کردن که الیوت، با توجه به شخصیت امنیت‌محوری که داره، نیازمند راهیه که بتونه فعالیت‌های ایمیلی‌اش رو نظارت کنه، و پرسیدن آیا پروتون‌میل از چنین امکانی پشتیبانی می‌کنه.

گزارش دسترسی حساب، که به پیشنهاد سازندگان سریال اضافه شد

و به این شکل، این امکان به پروتون‌میل اضافه شد. به لطف پیشنهاد بسیار خوب سازندگان مستر ربات، شما هم می‌تونید گزارش جامعی از فعالیت‌های حسابتون رو ببینید. اینجاست که می‌بینیم سطح توجه و تحقیق این تیم، چه در کار خودشون و چه در پروتون‌میل، چقدر تأثیرگذار بوده. الیوت دو سال بعد و در فصل سوم همچنان از پروتون‌میل استفاده می‌کنه، و جالبه که هر دو بار در قسمت هشتم فصل اتفاق افتاده.

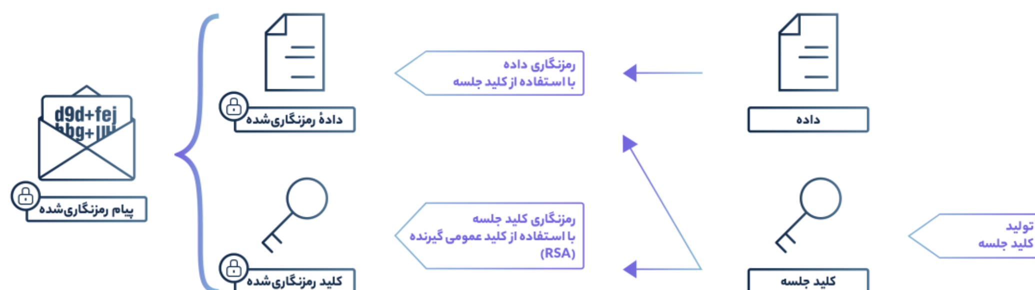
فکر می‌کنم آماده‌ایم تا به جزئیات رمزنگاری بپردازیم.

بهره‌مندی از PGP

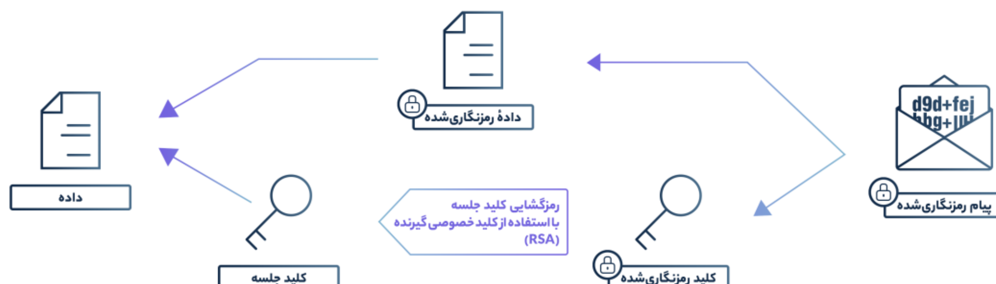
به‌طور خلاصه، پروتون‌میل از رمزنگاری PGP استفاده می‌کنه. درصورت عدم آشنایی با مفاهیم رمزنگاری، درک این بخش سخت خواهد بود. پیشنهاد می‌کنم ابتدا مطالب رمزنگاری کلید عمومی RSA و راهنمای جامع PGP رو مطالعه کنید و سپس به این بخش برگردید.

پروتون‌میل از ترکیبی از رمزنگاری متقارن و نامتقارن برای ارائهٔ رمزنگاری سرتاسر بهره می‌بره. وقتی کاربر حساب پروتون‌میل می‌سازه، مرورگرش یک جفت کلید RSA تولید و از کلید عمومی برای رمزنگاری ایمیل‌ها و سایر داده‌های کاربر استفاده می‌کنه. کلید خصوصی با گذرواژهٔ حساب رمزنگاری می‌شه.

رمزنگاری



رمزگشایی



اولین کاری که PGP انجام می‌ده تولید یک کلید جلسهٔ (session key) طولانیه. از این کلید برای رمزنگاری محتوای پیام (داده) استفاده می‌شه. کلید جلسه—که منحصربه‌فرده و با هر پیام تغییر می‌کنه—سپس با کلید عمومی گیرنده رمزنگاری می‌شه.

به زبان ساده‌تر، پیام رو با استفاده از رمزنگاری متقارن و به کمک کلید جلسه رمز و به متنی غیرقابل‌فهم تبدیل می‌کنیم. حالا یک دادهٔ رمزنگاری‌شده و یک کلید آشکار داریم. سپس، کلید جلسه رو با استفاده از رمزنگاری نامتقارن، با کلید عمومی گیرنده، رمز و برای او ارسال می‌کنیم. به شکل بالا توجه کنید.

گیرندهٔ پیام، که کلید خصوصی خودش رو داره، ابتدا کلید جلسه رو رمزگشایی و با کمک اون محتوای پیام رو باز می‌کنه—سریع، امن، و بدون‌دردسر.

چرا قدم اضافی؟ چرا داده رو مستقیم با کلید عمومی گیرنده رمزنگاری نکنیم؟ سؤال بسیار خوبیه.

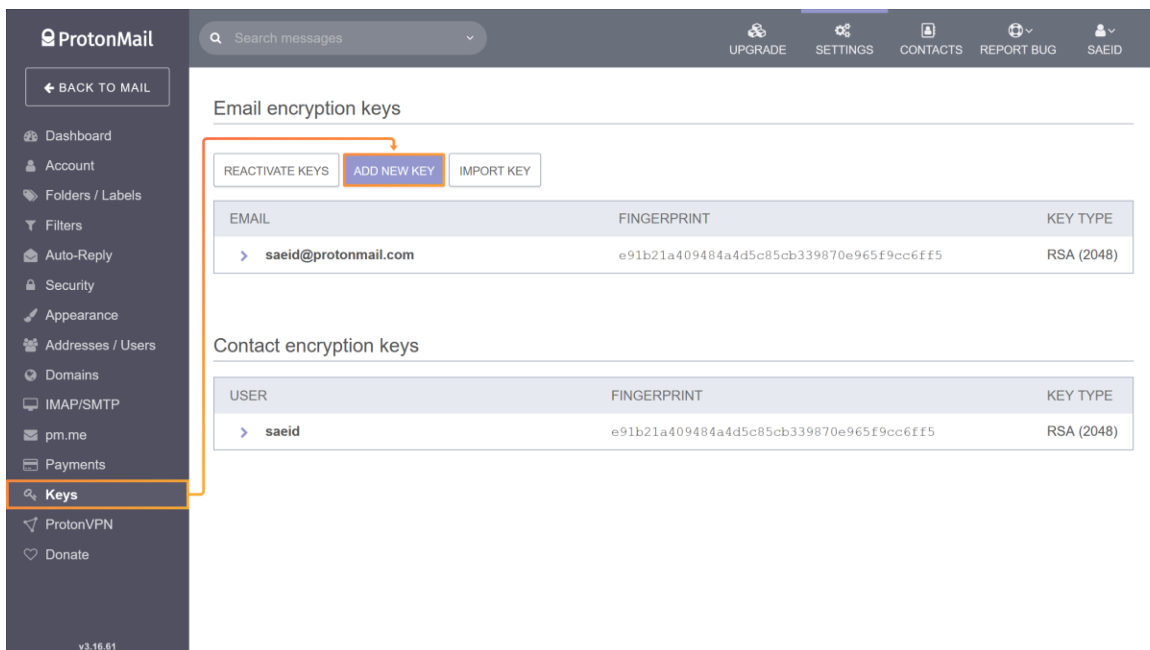
رمزنگاری کلید عمومی به‌طورکلی روش کندی محسوب می‌شه—بسیار کندتر از روش‌های متقارن. هرچقدر پیام و ضمیمه بلندتر و بزرگ‌تر باشه، رمزنگاری یا رمزگشایی اون‌ها زمان و قدرت پردازشی بیشتری می‌طلبه. روش فعلی سرعت و بهینگی رمزنگاری متقارن رو همراه با امنیت رمزنگاری کلید عمومی به ما می‌ده.

این روش دو جنبۀ دیگه هم داره، که قابل‌توجهه. در PGP با مفهوم امضای دیجیتال آشنا شده‌ایم. امضای دیجیتال این اطمینان رو به گیرنده می‌ده که پیامی که دریافت کرده حتماً از سمت فرستنده اومده. هر تغییری در پیام (یا کلید خصوصی امضاکننده) امضا رو نامعتبر می‌کنه.

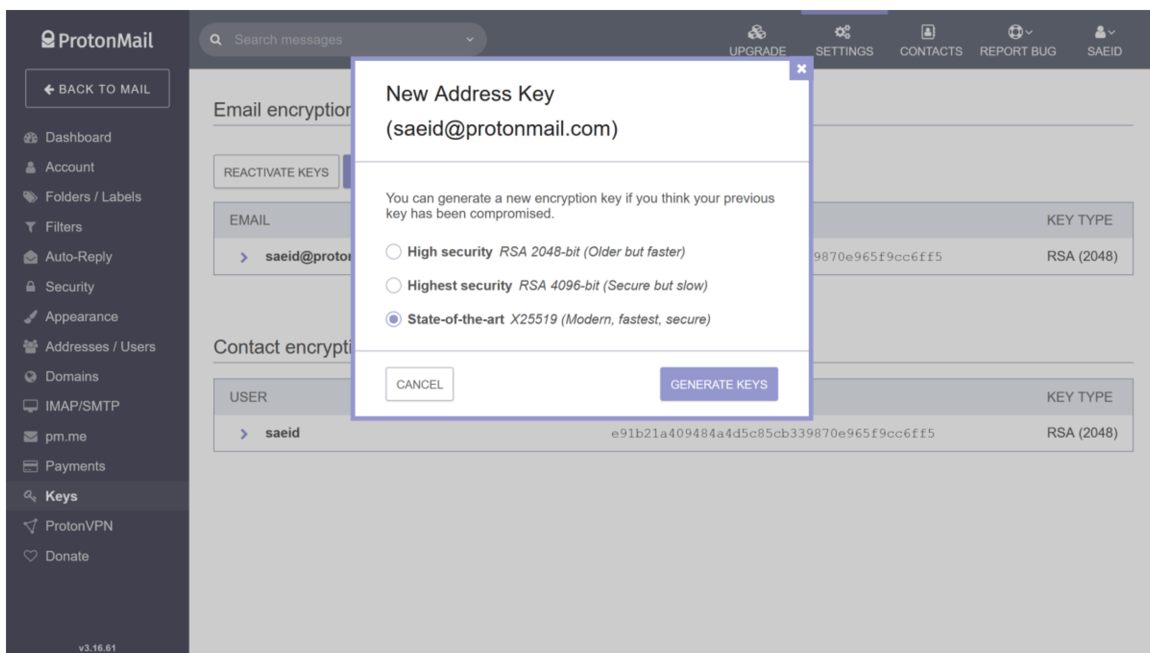
از طرفی، فرستنده چطور می‌تونه اعتماد کنه که کلید عمومی‌ای که برای رمزنگاری پیام و ارسالش به گیرنده استفاده می‌کنه به همون شخص تعلق داره؟ سرور می‌تونه یک کلید عمومی قلابی دراختیار فرستنده قرار بده. برای حل این مشکل، پروتون‌میل احراز آدرس (Address Verification) رو معرفی کرده. شما می‌تونید کلیدهای مخاطبین خودتون رو در پروتون‌میل به‌صورت دیجیتالی امضا—و اون‌ها کلید شما رو—و به این شکل به اون‌ها اعتماد کنید.
درحال‌حاضر، پروتون‌میل درحال کار روی امکانی با عنوان Key Transparency است، که کلید عمومی گیرنده‌ها رو خودکار احراز می‌کنه.

تغییر نوع کلید

درنظر داشته باشید که وقتی حساب می‌سازید، پروتون‌میل به‌صورت پیش‌فرض رمزنگاری RSA با کلید ۲۰۴۸ بیتی رو برای شما درنظر می‌گیره. شما می‌تونید کلید ۴۰۹۶ بیتی بسازید، یا از رمزنگاری منحنی بیضوی (ECC) برای سرعت بالاتری که ارائه می‌ده استفاده کنید. به تصاویر صفحات بعد توجه کنید.



قدم اول جهت افزودن کلید جدید با رمزنگاری منحنی بیضوی: Keys → Add New Key



قدم دوم: State-of-the-art → Generate Keys

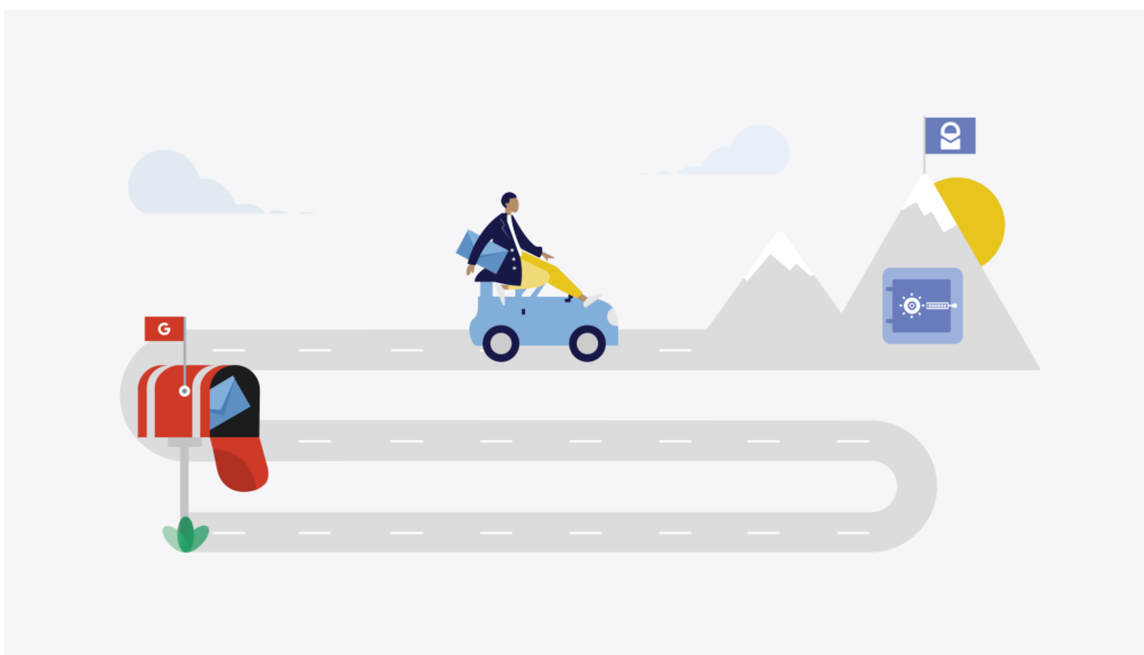
قدم سوم: انتخاب فلش کنار Export برای کلید تازه‌تولیدشده

قدم چهارم و آخر: انتخاب گزینهٔ Make Primary جهت استفاده از کلید تازه‌تولیدشده به‌عنوان کلید اصلی

برای مطالعهٔ جزئیات فنی رمزنگاری منحنی بیضوی به این مقاله رجوع کنید.

مهاجرت از سرویس‌های دیگه به پروتون‌میل

شما همچنین می‌تونید از سرویس‌های دیگه، مثل جی‌میل یا یاهو، به پروتون‌میل مهاجرت کنید، و نه‌تنها تمام ایمیل‌ها و فایل‌هاتون رو داشته باشید بلکه ایمیل‌های دریافتی در اون سرویس‌ها هم مستقیم به آدرس جدیدتون در پروتون‌میل فرستاده بشن. در این بخش به چگونگی این کار خواهیم پرداخت.



تصویر مقالهٔ How to migrate from Gmail to ProtonMail؛ بازطراحی‌شده توسط امیر آریا

برای انجام این کار در جی‌میل، ابتدا وارد تنظیمات جی‌میل شده و اطمینان حاصل کنید IMAP در بخش Forwarding فعاله. به Labels رفته و انتخاب کنید چه پوشه‌هایی رو می‌خواید انتقال بدید. به تصاویر صفحات بعد توجه کنید.

Gmail
Search mail
Compose
Inbox
Sent
Drafts
Trash
More
Meet
New meeting
Join a meeting

Settings

General Labels Inbox Accounts and Import Filters and Blocked Addresses
Forwarding and POP/IMAP Add-ons Chat and Meet Advanced Offline Themes

Forwarding: Add a forwarding address
Learn more

Tip: You can also forward only some of your mail by creating a filter!

POP download: **1. Status: POP is enabled** for all mail that has arrived since 12/23/11
Learn more
Enable POP for **all mail** (even mail that's already been downloaded)
Enable POP for **mail that arrives from now on**
Disable POP

2. When messages are accessed with POP
keep Gmail's copy in the Inbox

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
Configuration instructions

IMAP access: **Status: IMAP is enabled**
(access Gmail from other clients using
Enable IMAP
Disable IMAP

قدم اول: اطمینان از فعال‌بودن IMAP در بخش Forwarding

Gmail
Search mail
Compose
Inbox
Sent
Drafts
Trash
More
Meet
New meeting
Join a meeting

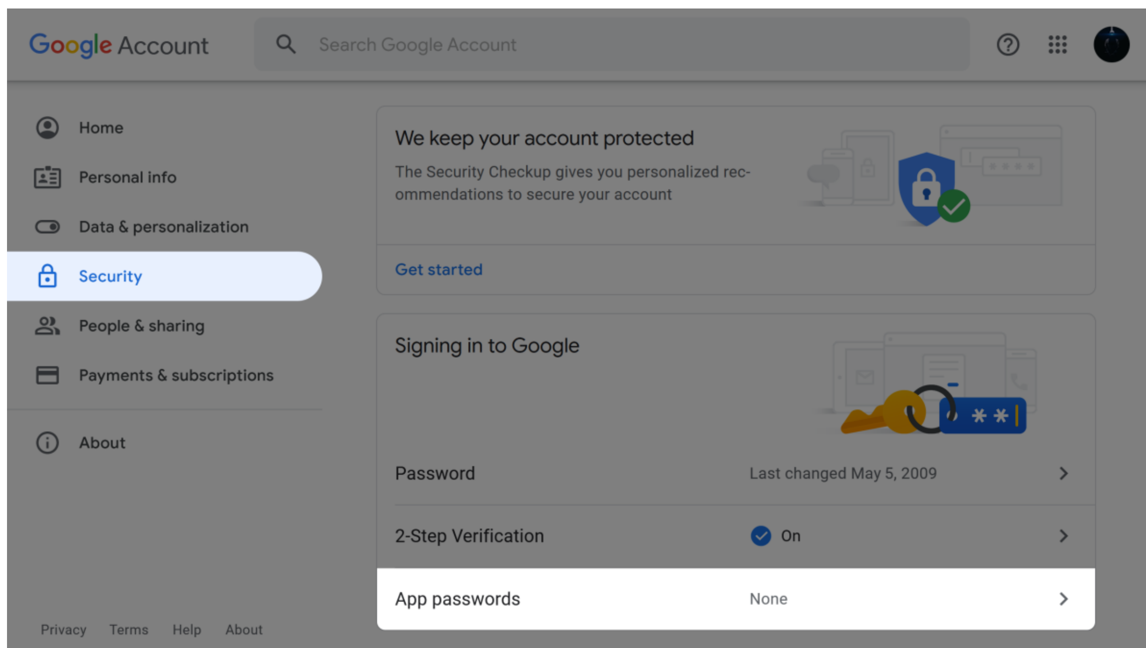
Settings

General Labels Inbox Accounts and Import Filters and Blocked Addresses
Forwarding and POP/IMAP Add-ons Chat and Meet Advanced Offline Themes

System labels	Show in label list	
Inbox		Show in IMAP
Starred	show hide	Show in IMAP
Snoozed	show hide	Show in IMAP
Important	show hide	Show in IMAP
Chats	show hide	Show in IMAP
Sent	show hide	Show in IMAP
Scheduled	show hide show if unread	Show in IMAP
Drafts	show hide show if unread	Show in IMAP
All Mail	show hide	Show in IMAP

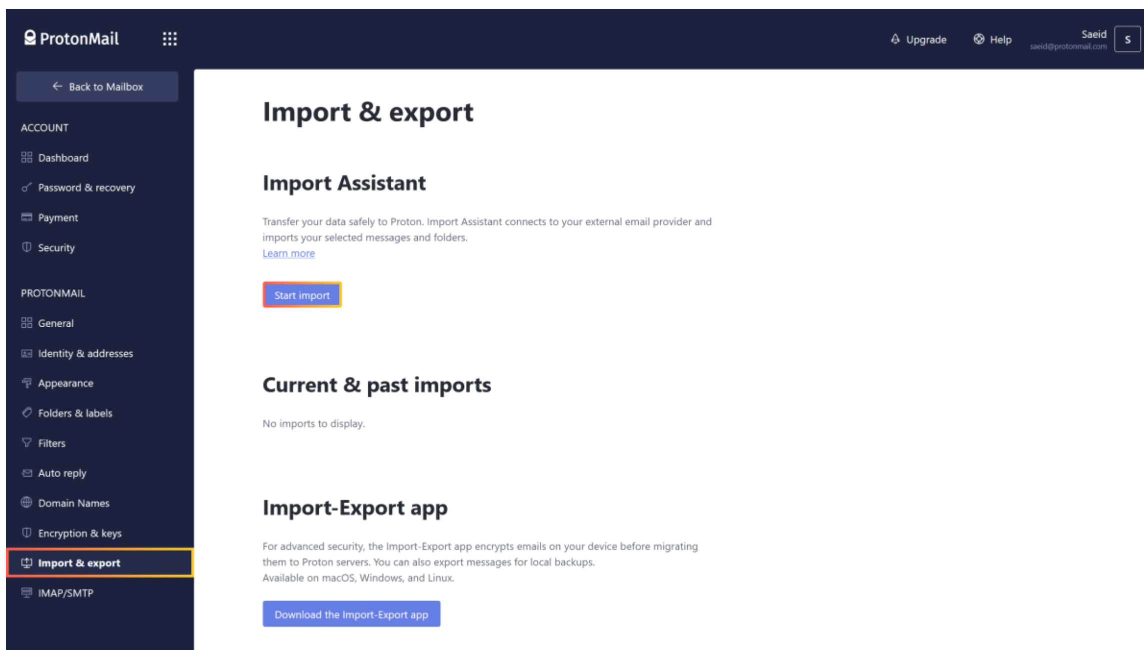
قدم دوم: انتخاب پوشه‌های موردنظر در Labels

حالا به تنظیمات حساب گوگل برید، در Security وارد App passwords بشید، و رمزی برای پروتون‌میل بسازید.

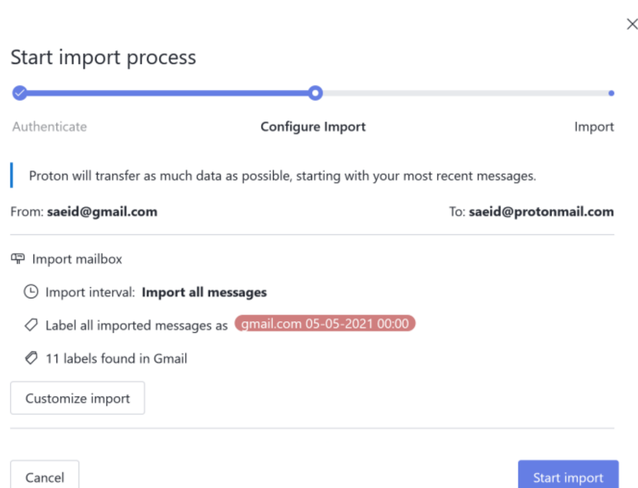


قدم سوم: تعیین رمز برای پروتون‌میل در Security → App passwords

اگه App passwords رو نمی‌بینید، به این دلیله که احراز دوعاملی (two-factor authentication) رو فعال نکردید، که در این حالت، توصیه می‌کنم اولین کاری که انجام می‌دید فعال‌کردنش باشه. درصورتی‌که احراز دوعاملی فعال نباشه، به جای App passwords گزینهٔ Turn on access رو خواهید دید.



در انتها، وارد سایت پروتون‌میل بشید، وارد حساب بشید، در تنظیمات به بخش Import Assistant برید (که در نسخهٔ بتا Import & export نام داشت)، و Start import رو بزنید. آدرس جی‌میل رو همراه با رمزی که در App Passwords گرفتید وارد کنید، و پروتون‌میل بقیهٔ کارها رو برای شما انجام می‌ده. یاهو هم روند مشابهی داره، اما اگه سؤالی بود، بپرسید.



قدم آخر: Import Assistant → Start import

درضمن، شما می‌تونید از آدرس‌های کوتاه‌شدهٔ pm.me@ هم استفاده کنید (به‌عبارتی، PM me یا بهم پیام خصوصی بده). هربار نوشتن protonmail.com می‌تونه سخت باشه، چه برای شما و چه شخص مقابل. برای این کار، به تنظیمات و بخش pm.me برید. کاربرهای مجانی فقط می‌تونن به این آدرس‌ها دریافت کنن.

بسیار عالی. با کلیات پروتون‌میل آشنا شدیم.

سخن پایانی

بالاتر به امنیت پایین ایمیل و ضرورت استفاده از آدرس‌های موقت اشاره کردیم. ابزار Firefox Relay رو برای این کار درنظر داشته باشید. همچنین، از یک ایمیل برای همهٔ ثبت‌نام‌ها استفاده نکنید.

برای ساختن حساب نیاز به واردکردن شمارهٔ تلفن ندارید، اما اگه سرویسی از شما درخواست کرد، توجه داشته باشید که این موضوع حریم خصوصی شما رو تحت‌تأثیر قرار می‌ده. درصورت‌نیاز از شماره‌های مجازی استفاده کنید.

اگه بخوام یک منبع معرفی کنم که اطلاعاتتون رو کامل کنه، ویدئوی ارائهٔ بارت باتلر مدیر ارشد تکنولوژی پروتون‌میله، که می‌تونید اون در Vimeo ببینید. در دقیقهٔ دوازده، جایی که داره درمورد تجربهٔ کاربری (UX) صحبت می‌کنه، نقل‌قول جالبی از بروس اشنایر (Bruce Schnier) میاره.

درنهایت، مهم‌ترین اصل اینه: DYOR (خودت تحقیق کن). پروتون‌میل بهترین نیست، اما گزینهٔ خوبیه. اشکال‌هایی بهش وارده، و خوبه که بدونیم اون‌ها چی‌ان. بدون‌شک پیشرفت‌های زیادی داشته، اما بی‌نقص نیست. درنتیجه، تنها به حرف من اتکا نکنید، به‌خصوص وقتی پای امنیت و حریم خصوصی درمیونه.

راهنماهای مرتبط



حریم خصوصی در عصر دیجیتال



فایرفاکس: حریم خصوصی، ابزارها، و ترفندها



